



الخدمة التي أوقفناها سيكم CRS-3



• 320 تيرا في الثانية

• أقوى 12 مرة من أقرب منافسيه

• تحميل محتوى الكونجرس في أقل من ثانية

نتائج الاستفتاء

هل أنت من متابعي مواضيع جونيير ؟

• نعم

38%

• لا

33%

• حسب الموضوع

28%



Juniper
NETWORKS

تعرف على جونيير
وعلى معداتها



تقرأون في هذا العدد

كيف يعمل الـ PING

Ping

الـ Port Security وهجوم

الـ Mac Flooding

كيف تحدد بأحترافية الفروق

بين IOS Image

لماذا نتجاهل وجود الـ

Subnet /31

والعديد من المواضيع

الجديدة والقيمة

شاهدوا أيضا أقسام

مصطلحات تقنية



عتاد ومعلومات



مشاكل وحلول



1



أفتتاحية العدد

العدد رقم واحد

المحررون الدائمون

- المهندس أيمن النعيمي
admin@networkset.net

المحررون الضيوف

- المهندس عثمان أسماعيل
othman_ucmael@yahoo.com

الحمد لله حمدا كثيرا على الطاقة التي أمدني بها لكي أحقق أول الأشياء الهامة التي أردت أن أقوم بها في حياتي وهي إنشاء أول مجلة عربية تختص بأمور الشبكات وتوابعها .

بدأت فكرة إنشاء المجلة أول مرة من خلال طلب بعض الأصدقاء لي أن أقوم بتحويل المواضيع والشروحات التي أقوم بها إلى ملفات بي دي أف لكي يسهل عليهم الرجوع إليها وقت الحاجة وبعدها بدأت تتكون عندي أسباب أكثر تدفعني إلى القيام بتأسيس مجلة تحوي كل المواضيع والمقالات المهمة التي أقوم بكتابتها ومن بين هذه الأسباب :

أ- نشر المعرفة في كل مكان تستطيع المجلة الوصول إليه

ب- تشجيع هذا النوع من المجلات للانتشار في الوسط العربي

ج- حتى أبتعد عن متابعة عداد الزوار في المدونة يوميا

وتتركز أهداف هذه المجلة بشكل أساسي في نشر المواضيع التي تشكل الحجر الأساس في مفاهيم الشبكات وتطبيقاتها وبعيدا عن فكرة نشر الأخبار الجديدة التي يمكن الاطلاع عليها في كل مكان كما أحب أن أوجه دعوة لكل شخص متمكن وقادر على الكتابة أن يشاركني هذا العمل البسيط من خلال إرسال المقالات المفيدة في عالم الشبكات أيا كان نوعها وبدوري سوف أخصص للمجلة عامودان رئيسيان الأول يتضمن المحررون الدائمون والثاني سوف يكون للمحررون الضيوف في هذا العدد .

كما أرحب بأي اقتراحات أو إضافات تساعد في تطوير المجلة بشكل أفضل وهذا يشمل إضافة أقسام جديدة أو طريقة تصميم المجلة لان حاولت جاهدا أن أقوم بتصميم المجلة بأفضل صورة ممكنة وإن لم تصل إلى المستوى الذي طمحت إليه بسبب خبرتي البسيطة في برامج التصميم .

وأخيرا ن كان هناك خطأ فهو من نفسي ومن الشيطان وان كان هناك فائدة فهي من فضل الله عليّ وعليكم ولا أطلب منك إلا الدعاء لي ولوالداي وبالقوة لآتمام هذا العمل البسيط .

موقع المجلة

www.networkset.net

بريد المجلة

magazine@networkset.net

بريدي الخاص

admin@networkset.net

محتويات نيسان 2110



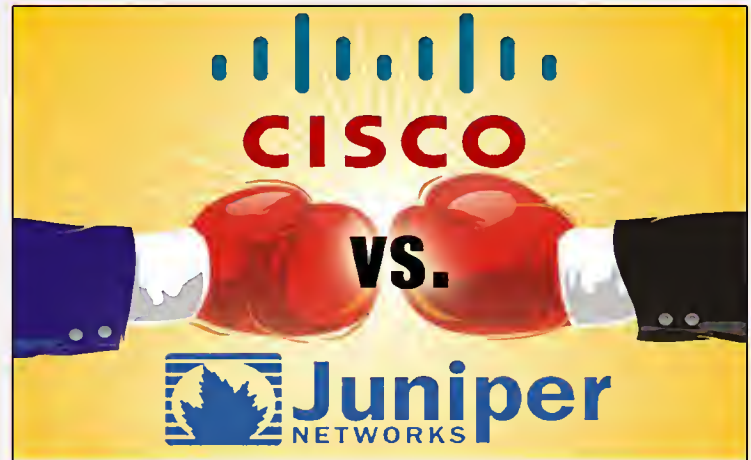
تعرف على منتجات جونيپر صفحة رقم 3

- 14 - تعرف على كيفية كتابة الأوامر في جونس
- 15 - حقيقة الـ 31 / Subnet
- 15 - Default Interface
- ماذا سوف يختار الروتر لو كن لديه بروتوكولان مختلفان
- 16 - لهم نفس AD
- كيف تقوم بعمل Load balancing في ويندوز
- 16



الخدعة التي أوقعتنا بها سيسكو صفحة رقم 8

- 5 - كيف يعمل الـ PING من منظور الشبكات
- 6 - ماذا علي أن أختار DTE أو DCE
- 7 - تعرف على جميع أنواع الشبكات الموجودة
- 9 - أنتل و سيسكو تصدران كروت الشبكة لسرعة 10 غيغا
- 9 - مجلة Fortune تختار سيسكو للمرة الثالث عشرة
- 10 - كيف تختار نسخة سيسكو IOS المناسبة
- 13 - نتائج الاستفتاء



مقارنة بين سيسكو وجونيپر صفحة رقم 12

- قسم الأمن والحماية
- 17 - هجوم Mac Flooding وطريقة التصدي له
- 18 - الـ ROMmon سلاح ذو حدين
- 19 - قسم عتاد ومعلومات
- 21 - قسم مصطلحات تقنية
- 22 - قسم مشاكل وحلول



Juniper® NETWORKS

تُعرف على جونيپر وعلى عائلته

بقلم أيمن النعيمي



بعد طرحي لبعض المواضيع حول جونيپر وجدت أن الأغلبية مازالت تجهل هذه الشركة العملاقة التي أصبحت تحتل المرتبة الثانية في عالم الشبكات بشكل عام والمرتبة الأولى في الأمن والحماية على مستوى العالم في الشبكات بحسب بعض الأحصائيات لذلك قررت اليوم أن أقوم بعرض بسيط حول هذه الشركة ومنتجاتها رغبتا مني في زيادة المدخول العربي حول هذه الشركة.

مقدمة عن شركة جونيپر

بدأت جونيپر برأس مال محدود حوالي 200 ألف دولار ولتحصد بعد عام واحد من تأسيسها حوالي 60 مليون دولار من أكثر من شركة عالمية مثل 3COM, AT&T وفي عام 1998 أعلنت جونيپر عن أول منتج لها M40 router وكان أول منتج على مستوى العالم يستحدث تقنية نقل البيانات مستخدما السليكون (ASICs) وقد فتحت هذه التقنية للأنترنت بالنمو بشكل كبير بفضل السرعة الكبيرة التي أتاحتها ولتدخل شركة جونيپر عالم الشبكات من أوسع أبوابه ولتقضي على هيمنة سيسكو الطويلة.

أستمدت جونيپر أسمها من شجر صنوبري يطلق عليه العرعر الذي تشتهر فيه مدينة كاليفورنيا الأمريكية وهو المكان الذي ولدت فيه هذه الشركة أول مرة. تأسست جونيپر في شباط عام 1996 بواسطة 3- أشخاص هم:

Pradeep Sindhu المدير الفني في الشركة والذي كان حينها يشغل منصب هام في شركة Xerox

Dennis Ferguson خبير شبكات من شركة MCI

Bjorn Liencres خبير فني في مجال العتاد والتصميم من شركة SUN

T-series : Core Platforms



تم تصميم هذه الفئة لتعمل كنواة أساسية للشبكة بطاقة كبيرة جداً تبدأ من 320 غيغا بت لتصل إلى 25.6 تيرابت في الثانية الواحدة وتتضمن هذه الفئة الموديلات التالية :
T320, T640, T1600 TX Matrix, TX Matrix Plus
وجميعها تعمل تحت نظام JUNOS

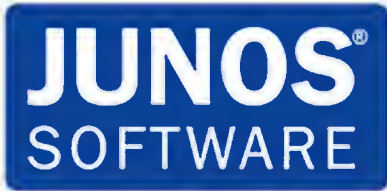
منتجات السويتش

للسويتش هناك فئة واحدة وهي

EX-series



والتي أراها من أكفء السويتشات في العالم برائي الشخصي لما تتمتع من مميزات مثل مميزات Virtual Chassis في سويتشات EX-4200 بالإضافة إلى 4 موديلات أخرى هي: EX2200, EX2500, EX3200, EX8200 تختلف فيما بينها بعدد البورتات وبسعة نقل البيانات وبعض المميزات الأخرى.
وجميع موديلات هذه الفئة تعمل تحت نظام



صورة لأول منتج من جونيبر روتر R40



تعد هذه الفئة من الأنواع الكبيرة والمخصصة للشركات التي تتطلب أداء عالي في عملها بالإضافة لخدمي الأنترنت وتتضمن الموديلات التالية: M7i, M10i, M40e, M320

وهي تتيح للشركات ومخدي الأنترنت بربط عدة شبكات فرعية بروتر واحد مما يعطيك مرونة وأداء كبيران كما تصل سرعة النقل إلى (320 غيغا) حسب الموديل . بالإضافة إلى دعمها العديد من تقنيات ال WAN مثل Ethernet, ATM, SONET والكثير...
وهي معدة أيضاً لكي تعمل تحت نظام JUNOS

MX-series: Ethernet Services Routers



تعد هذه الفئة موجهة بشكل عام لخدمي الأنترنت وكما هو واضح من الاسم تعد هذه الفئة من الفئات التي تدعم خدمات Ethernet بشكل كبير لتصل سرعة النقل فيها إلى 960 غيغا بت كل ثانية كما هو الحال في الموديل رقم MX960

أما موديلات هذه الفئة فهي : MX80, MX240, MX480, MX960 وقد تم تطوير هذه الفئة من الروترات في عام 2009 إلى الجيل الجديد تحت اسم MX-3D بالإضافة المزيد من ال Slot إليها بهدف تحسن الأداء أكثر من قبل.

وفي صيف عام 1999 دخلت جونيبر سوق الأسهم العالمية ناسداك بسعر 34 دولار للسهم الواحد ولتبيع أكثر من 4 مليون سهم مقدماً وليلصل سعر السهم بعد عام واحد إلى 240 دولار (شيء خيالي)

هذه لمحة بسيطة عن تاريخ بداية هذه الشركة ورغبة مني في التركيز أكثر في المنتجات ولعرفة تفاصيل أكثر عن جونيبر في هذا المضمار تستطيع أن تدخل على موسوعة ويكيبيديا العالمية على الأنترنت للتعرف أكثر عليها

وكحال أي شركة تعمل في مجال شبكات الحاسب تملك جونيبر الكثير من المنتجات التي أراها متقدمة بعض الشيء والتي عادة تستهدف الشركات الكبيرة ومخدي الأنترنت وهو السبب الرئيسي في رأيي في عدم انتشارها في عالمنا العربي بالشكل المطلوب بعكس منتجات سيسكو التي تغطي جميع فئات ومتطلبات العمل

لنبدأ الآن التعرف على منتجات جونيبر.

منتجات الروتر

للوتر عدة فئات مختلفة بالحجم والأداء.

وسوف أبدأ بالفئات الأصغر حجماً

J-series: Services Routers



تتضمن هذه الفئة من الروترات الموديلات التالية: J2320, J2325, J4350, J6350 وتتمتع بمرونة وأداء عالي تناسب الشبكات الصغيرة وتعمل جميع أنواع هذه الفئة تحت نظام JUNOS الذي تم تطويره في معالج جونيبر الخاصة.

كما تدعم هذه الفئة العديد من الخدمات المتقدمة مثل MPLS, IPv6, QoS, Multicast وفي مجال الأمن تحتوي هذه الأنواع على جدار ناري مدمج بالإضافة لبعض الخدمات مثل VPN, IPsec وزد على ذلك إمكانية تطوير العتاد في حال زيادة الأداء في المستقبل.

M-series: Multiservice Edge Routing Portfolio



هذا كل مايجبتي الآن كمحاولة بسيطة منى لتغطية منتجات شركة جونيبر العملاقة في الروتر والسويتش وأن شاء لي عودة في المستقبل القريب لتغطية منتجاتها في الأمن والحماية. وللتعرف بشكل أكبر على مميزات كل موديل من هذه الموديلات تستطيع الدخول على هذه الروابط التالية :

WWW.JUNIPER.NET/US/EN/PRODUCTS-SERVICES
WWW.NETSCREEN.COM/PRODUCTS_AND_SERVICES

كيف يعمل الـ Ping؟

مامو الـ Ping؟

Ping بشكل عام هو عبارة عن أداة تستخدم بروتوكول الـ ICMP أو Internet Control Message Protocol وللذين يجهلون عمل هذا البروتوكول أقول لهم هو عبارة عن بروتوكول يعمل في الطبقة الثالثة Network Layer وهو مسؤول عن إرسال رسائل الأخطاء في الشبكة بشكل عام

ماذا يحدث عندما نقوم بإرسال Ping إلى أحد الأجهزة؟

في بداية الإرسال يقوم بروتوكول الـ ICMP بإرسال Echo Requests وهي أحد وظائف البروتوكول ويتم التعبير عنها في الـ Header بالقيمة التالية 8, Type 0 Code طيب سوف تقول لي لم أفهم شيء؟

لننظر أولاً إلى الجدول التالي ولنكمل الشرح بعدها

Type	Code	Description
0	0	Echo reply (تخبر لرد على الطلب)
	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
3	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Source host isolated
	8-13	موجود لكن غير مهمة جداً
4	0	Source quench
	0	Redirect Datagram for the Network
	1	Redirect Datagram for the TOS & network
5	2	Redirect Datagram for the TOS & network
	3	Redirect Datagram for the TOS & host
6	0	Alternate Host Address
8	0	Echo request (نستخدم الطلب)
9	0	Router Advertisement
10	0	Router discovery/selection/solicitation
11	0	TTL expired in transit
	1	Fragment reassembly time exceeded
	2	Pointer indicates the error
12	1	Fragment reassembly time exceeded
	2	Bad length
13	0	Timestamp
14	0	Timestamp reply
15	0	Information Request
16	0	Information Reply
17	0	Address Mask Request
18	0	Address Mask Reply

بعد اطلاعنا على هذا

الجدول والذي يسمى

جدول الـ ICMP لنضع أمامنا

الـ Header الخاصة بي الـ

Packet المرسله ولنربط الأفكار مع بعضها البعض

ICMP Echo Request		
Type = 8	Code = 0	Header Checksum
Identifier		Sequence Number
Data		

الخلاصة

عند إرسالنا للطلب أو التحقق من الأيبي المطلوب يقوم الـ ICMP بتحديد الـ Type ثمانية وهي يدل على أن هذه البايت هي للطلب أما بالنسبة للكوند فهو صفر لأن هذه الوظيفة لا تملك خيارات ثانوية بعكس رقم الـ 3 Type وهو المسؤول عن فشل عملية الـ Ping ونجد في خانة الـ Code هناك عدة خيارات تدل على سبب الفشل بالضبط

ونستنتج أن خانة الـ Type تحدد نوع الرسالة في بروتوكول الـ ICMP بينما خانة الـ Code تستخدم إذا كان هناك خيارات متاحة في هذا النوع من الرسائل

أما بالنسبة لباقي الخانات في الـ Header فهي تقريبا معروفة عند الجميع وهي على الشكل التالي :

موضوعنا بالمسمى بسيط لكن فهمه مهم لكل شخص محترف يعمل في مجال الشبكات لأنه يعد من أهم الأدوات التي تساعدك في تشخيص الكثير من المشاكل التي تتعرض لها أثناء العمل وأنا أتوقع أن كل واحد فينا سأل نفسه هذا السؤال : كيف يعمل الـ Ping ؟

وطبعاً محور حديثنا لن يكون عن برمجة الـ Ping أو شرح كيفية الاستفادة منه ومن أوامره .

الموضوع ببساطة سوف يلخص كيفية عمل الـ Ping من منظور الشبكات

لنبدأ أولاً بالتعرف على ماضي الـ Ping

الـ Ping تم كتابته لأول مرة عام 1983 من قبل Mike Muuss وتم تسميته على مبدأ جهاز "السونار" الذي يستخدم في السفن بهدف تحديد مواقع الغواصات عن طريق إرسال نبضات صوتية.

ولتفهم الموضوع بشكل جيد يتطلب هذا منك

خلفية بسيطة في مفهوم الطبقات و TCP/IP.

استخدام الـ Ping

كما نعلم جميعاً أننا عندما نريد أن نقوم

بعمل Ping نبدأ أولاً بكتابة كلمة Ping

وبعدها نضيف اسم الموقع أو الأيبي المراد

عمل التجربة عليه وتكون النتيجة على الشكل ا

لتالي

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ayman_bat>ping networkset.wordpress.com

Pinging 1b.wordpress.com [74.200.243.251] with 32 bytes of data:

Reply from 74.200.243.251: bytes=32 time=181ms TTL=50
Reply from 74.200.243.251: bytes=32 time=181ms TTL=50
Reply from 74.200.243.251: bytes=32 time=182ms TTL=50
Reply from 74.200.243.251: bytes=32 time=180ms TTL=50

Ping statistics for 74.200.243.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milliseconds:
        Minimum = 180ms, Maximum = 182ms, Average = 181ms
C:\Documents and Settings\ayman_bat>
```

تدلياً الصورة السابقة على نجاح العملية بينما تدلياً الصورة القادمة على فشل العملية

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ayman_bat>ping 95.122.58.56

Pinging 95.122.58.56 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 95.122.58.56:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings\ayman_bat>
```


القطعة الأخيرة وهي الـ TTL

أكثر معضلة واجهتهما في هذا الموضوع والأجابات تعددت من خلال بحثي في الإنترنت وفي غوغل فمنهم من يقول هي عدد الهوب للوصول للمدف وهناك من يقول هي الوقت الذي يستغرقه الطلب للوصول للمدف وبعد البحث والتجربة توصلت الى انهما قيمة تحدد من قبل كل روتر

أو أي جهاز وسيط وهي تزيد أو تنقص حسب مسار البايت الى المدف وكمثال على ذلك قم بعمل Ping 127.0.0.1 أي لوبباك على الجهاز لوجدتها 128 وهذا يعني أن قيمة الـ TTL في ويندوز تساوي 128 بينما القيمة في لينوكس تساوي 64 وهي تبدأ بي 256 وتتناقص مع مرورها بالجهاز الوسيط وللتأكد من هذا الموضوع قمت بهذه التجربة الصغيرة

Ping -i 5 networkset.net

وكما هو موضح انا قمت بتحديد الـ TTL بي 5 والنتيجة كانت على الشكل التالي

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ayman_bat>ping -i 5 networkset.wordpress.com
Pinging lb.wordpress.com [76.74.254.123] with 32 bytes of data:
Reply from 213.242.109.34: TTL expired in transit.
Reply from 213.242.109.34: TTL expired in transit.
Reply from 213.242.109.34: TTL expired in transit.
Reply from 213.242.109.34: TTL expired in transit.

Ping statistics for 76.74.254.123:
    Packets: Sent = 4, Received = 0, Lost = 0 (0% loss),
    approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\ayman_bat>
```

لم يستطيع الطلب الوصول للمدف لان قيمة الـ TTL كانت غير كافية

Header Checksum: المسؤولة عن error detection
Identifier: وهي في الاغلب تكون 256 وهي تحوي على processID
Sequence Number: تبدأ بصفر وتزيد مع عدد مرات الطلب Echo
طبيب السرطان الذي كيف تتم عملية الرد

الجواب ابسط بكثير بعد ما فهمنا كيفية الطلب لان الموضوع ببساطة سوف يكون نفس الشيء مع تغيير خانتي الـ Type والـ Code وسوف تكون محتويات الـ Header كالتالي

ICMP Echo Reply		
Type = 0	Code = 0	Header Checksum
Identifier		Sequence Number
Data		

سوف نلاحظ ان العملية ناجحة والطلب قد تم لاننا نرى ان الـ Type يحمل الرقم 0 وبمراجعة الجدول سوف نجد انه يدل على ان العملية تمت والهدف قام بالرد على الطلب

لكن لو عرضت عليك هذا الجدول ماذا برئيك سوف يحدث ؟

ICMP Echo Reply		
Type = 3	Code = 1	Header Checksum
Identifier		Sequence Number
Data		

الجواب طبعا سوف يكون ان عملية الطلب لم تتم والسبب عدم القدرة على الوصول للمدف (راجع الجدول)

ماذا عليا أن أختار

DTE

DCE

تستطيع تجربتها على برنامج البايت ترايسير وذلك من خلال اعداد الـ Clock Rate فقط على منفذ الـ DCE وبعدها اتجه الى الطرف الأخرى الروتر الثاني وسوف تجد أن الروتر قد حصل على الأعداد نفسه للـ Clock Rate من الطرف الأول

لنأخذ مثال من نوع آخر لنفرض أن الإنترنت عندما يعمل من خلال DialUp Modem فعندما تريد الاتصال بالإنترنت تقوم بكتابة رقم الهاتف وأرساله إلى كرت المودم وهو بدوره يقوم بالاتصال بالإنترنت اذا المودم هنا يلعب دور الـ DCE لانه هو من يقوم بتجهيز الاتصال مع مخد الإنترنت بينما جهاز الكمبيوتر يلعب دور الـ DTE

وهذا الفرق أيضا نلاحظه عندما نقوم بالاتصال بالروتر من خلال الكونسول بورت لان نجاح الاتصال بين الروتر والكمبيوتر يتطلب منك أن تقوم بأعداد الـ Boud Rate لكي تتلائم مع الروتر ولاحظ اني لا أقول أعداد الروتر ليتلائم مع جهاز الكمبيوتر لان الروتر هنا يلعب دور الـ DCE بينما جهاز الكمبيوتر أو الأفضل قول معالج الكمبيوتر هو دائما DTE

خلاصة هذا الكلام هو أن الـ DCE يلعب دور المرسل بينما الـ DTE يلعب دور المستقبل

مرات كثيرة أنطرح علي سؤال وهو الفرق بين الـ DTE والـ DCE ؟
وسبب طرح هذا السؤال بشكل متكرر هو استخدام البعض لبرنامج البايت ترايسير والذي يتيح لك أن تقوم بوصل الروترات ببعضها عن طريق مايعرف بي الـ Serial Port والذي يتيح بدوره نوعان من أسلاك التوصيل DTE serial أو DCE serial

لنتفق أولا على معنى كل واحد فيهم

DTE وتعني Data Terminal Equipment

DCE وتعني Data Communication Equipment

ومما لا شك فيه أن هذه التعريفات لا تقتصر فقط على الروترات لان كوابل السيرال موجودة في كل مكان مثل الكابل الموصول بين جهاز الكمبيوتر والمودم وبين جهاز الكمبيوتر والطابعة وبين جهاز الكمبيوتر وشاشة العرض والـ ...

لنعد إلى السؤال الرئيسي DTE or DCE ؟

تنقسم الأجهزة التي تدعم خاصية النقل بواسطة السيرال إلى نوعين إما DTE أو DCE أو الاثنين مع بعضهم ويمكن الفرق الرئيسي بينهم هو أن الـ DCE مسؤولة عن عملية أعداد الاتصال نفسه فكما نعلم أن استخدام السيرال بورت يتطلب منك أعداد Clock Rate واحدة على كلا الطرفين

ومن هنا تأتي فائدة الـ DCE فهي تقوم بأرسال معلومات الـ Clock Rate التي تم أعدادها على هذا المنفذ إلى المنفذ الآخر وهذا يفسر وجود رمز الساعة في برنامج البايت ترايسير
لأيجاء لك أن هذا الطرف سوف يكون المسؤول عن عملية

Type of network

Wan	Man	Can
Lan	Pan	San
Gan	Wlan	Network Set

أثناء إعطائي لأحد كورسات الشبكات سألت الطلاب سؤال بسيط جدا في الشبكات ماهي أنواع الشبكات الموجودة والأجوبة كان أغلبها أن للشبكات هناك نوعين Lan & Wan وهناك من أضاف أيضا بوجود شبكات الوايرليس وطبعا هذه الأجوبة كلها صحيحة ومعروفة عند الجميع لكن الحقيقية أن للشبكات أنواع كثيرة وقد تسمح بها لأول مرة فهناك Wan, Lan, Man, Pan, Wlan, Can, San and Gan

لنتعرف على شرح مبسط لكل نوع

Metropolitan area network (MAN)

من حيث المدى يعد هذا النوع هو الوسط بين الـ Lan و Wan فهو أطول من الـ Lan وأقصر من الـ Wan ويستخدم هذا النوع في وصل الشبكات المحلية ببعضها البعض من خلال روترات أو سويتشات وضمن نطاق محدود مثل نطاق المدينة ويستخدم هذا النوع تقنيات متنوعة مأخوذة من الـ Lan أو Wan بحسب المسافة والمكان الجغرافي للشبكة لذلك نجدها أحيانا تستخدم الـ Ethernet أو الـ ATM أو الخ

Wide area network (WAN)

يستخدم هذا النوع من الشبكات للمسافات البعيدة المدى مثل أن نصل مدينتان ببعضهما البعض أو أن نصل دولتين ببعضهم ويستخدم هذا النوع أحد التقنيات التالية Frame Relay, ATM, X.25 وسرعته تبدأ من 2-ميغا وتصل إلى 650 ميغا وقد تزيد أحيانا مع التطور الطبيعي للشبكات

Local area network (LAN)

أكثر أنواع الشبكة شهرة والسبب لاننا في حياتنا العملية نتعامل معها بشكل دائم ويستطيع هذا النوع من الشبكات أن يغطي مساحة جغرافية محدودة جدا أي على مستوى شركة أو منزل أو جامعة أو بناء مكون من عدة أدوار ويستخدم هذا النوع في أغلب الأوقات تقنية الأيثرنت والكوابل العادية للاتصال بين الأجهزة وسرعته تتراوح بين 10-100-1000 ميغابت

Campus area network (CAN)

من حيث المدى يعتبر هذا النوع هو الوسط بين شبكات الـ Lan و Man فهو أقصر من الـ Man وأطول من الـ Lan ويستخدم عادة لوصل شبكات داخلية محدودة جدا أي ضمن منطقة واحدة مثل أن نصل مبنيين مع بعضهم البعض أو أن نصل عدة جامعات موجودة في حرم جامعي واحد ويستخدم نفس التقنيات المستخدمة في الـ Lan

Wireless local area network (WLAN)

من أنواع الشبكات المعروفة أيضا وتستخدم موجات الراديو للاتصال بين بعضها البعض ولها ترددات معروفة مثل 2.4, 5.0 GHz وسرعته تتراوح بين 2ميغا إلى 54ميغا وتستخدم تقنية الـ DSSS و OFDM ولها 3-أنواع من الاتصالات, IBSS, BSS ESS

Personal area network (PAN)

هذا النوع من الشبكات مسافتها لا تتعدى الـ 10-أمتار وتستخدم أحيانا للوصل بين جهازين كمبيوتر أو جهاز كمبيوتر مع فاكس أو جهاز كمبيوتر مع طابعة وتستخدم في أغلب الأحيان تقنية الـ Bluetooth أو Infrared أي أن الاتصال يتم بشكل لاسلكي باستخدام الموجات اللاسلكية

Storage area network (SAN)

هذا النوع من الشبكات يصل السيرفرات مع مركز المعلومات الرئيسي data storage center ويستخدم تقنيات عالية في السرعة مثل تقنيات الفايبر

Global area network (GAN)

هذه النوع من الشبكات يستخدم عادة في الاتصالات لربط شبكات الموبايل ببعضها البعض مثلا و يستخدم هذا النوع الاتصالات اللاسلكية أو عن طريق الأقمار الصناعية

كلمة أخيرة الموضوع هدفه فقط التعريف بأنواع الشبكات المتاحة وأعطاء نظرة مبسطة عنها لأن كل نوع من هذه الشبكات يحتاج مواضيع لشرحه والتعرف عليه وهذا ما سوف أتركه لك لكي تتعلمه بنفسك

خدمة سيسكو في CRS-3

بقلم: أيمن النعمي



هكذا أعلنتها سيسكو على الملأ التقنية التي سوف تغيير عالم الانترنت أو الجيل الجديد من الانترنت هو CRS-3

فتح الامكانيات التي تحدث سيسكو عنها في هذا النوع من أجهزة الروتر وأن كنت لا أفضل أن أقول عنها روتر فهي بالنسبة لي ديناصور يشنح الانترنت تقوم بإرسال رسالة إلى كل مصنعي أجهزة الشبكات في العالم وأن كانت تخص شركة جونيبر بالتحديد والتي كانت تملك أقوى جهاز في العالم والمعروف بي Matrix باستطاعة 25-تيرا بت في الثانية بينما الـ CRS-3 أقوى منه بي 12-مرة وقدرة نقل البيانات فيه تصل إلى 320-تيرا بت في الثانية وللذين يجهلون معنى هذا الرقم في الحياة العملية فهي تمثل استطاعة تحميل كل الأفلام التي تم إنتاجها في هوليوود في مدة زمنية لا تتعدى الأربع دقائق أو السماح لجميع سكان الصين بأجراء مكالمة عبر الفيديو في نفس الوقت.

سوف لن أخوض كثيرا في تفاصيل هذه التقنية لأن المواضيع التي كتبت عنها كافية ووافية ولنتكلم في النقطة الأهم وهي الخدمة الكبيرة التي قامت سيسكو بترويجها

فعندما أعلنت سيسكو أن استطاعت هذا الجهاز تصل إلى 320-تيرا بت وربطتها ببعض الأمثلة الخيالية التي جذبت الجميع للوقوع في هذه الخدمة لتبعد القارئ عن الحقيقة الأساسية وهي أن هذه الاستطاعة لاتأتي من جهاز مركزي واحد فكما هو واضح عندكم من الصورة أن هذا الجهاز عبارة عن multichassis وله 3-أقسام قامت سيسكو بجمع إمكانيات كل واحد فيهم لتعلن عن هذا الرقم الخيالي والذي بدوره يقودنا إلى استنتاج أن قدرة هذا الجهاز أقل مما هو عليه ؟

ويرتكز هذا الاستنتاج على حقيقة واحدة وهامة وهي معروفة عند الخبراء تقول كل ما زاد عدد الـ Slot زادت استطاعة الروتر لنقل البيانات لأن الوصول إلى قدرة 320-تيرا بت يحتاج منك توصيل 72 chassis مع بعضها البعض للوصول إلى هذا الرقم وسيسكو كما هو واضح من الصورة قامت بعمل منتج كبير جدا يتألف من 3-أراكات ومع وجود معالج مثل QuantumFlow الجديد من سيسكو سوف نحصل على مثل هذه القدرة الهائلة وأن كنت لا أعلم كم عدد المعالجات التي تم إضافتها لهذا المنتج والتي لا أستبعد أن تكون كثيرة جدا .

حتى نظام التشغيل الذي يعمل فيه هذا المنتج IOS-XR والذي يصنف من فئة Modular operating system تم أخذ فكرته الأساسية من جونيبر التي تستخدم هذه النظام منذ بداية عصرها

وباختصار الحسابات التي أدخلتها بها سيسكو غير دقيقة أبدا لأن حساب استطاعة أي منتج يجب أن تكون حسب الخصوصية وبمعنى آخر العملية لاتتم بصف 3-منتجات ببعضها البعض والتحدث عنها كأنها هيكل واحد وتؤدي عملا واحدا لذا دعونا ننتظر بدء تسويق هذا المنتج الذي سوف يكشف كل الحقائق الخفية وأن كانت سيسكو لم تعلم عن أي موعد لبدأ بيع هذا المنتج والتي توحي لي بأن سيسكو أرادت أن توجه عدسات التصوير ومواقع الأخبار إليها مجددا وعلى قولة أخواننا في مصر ياخير اليوم بفلوس بكره يبقى يبلش.....

نتيجه هام: هذه استنتاجات شخصية فقط من باب المنطق العام ولا يوجد أي

مصدر لها

أخبار متنوعة

مجلة FORTUNE تختار سيسكو للمرة الثالثة عشر

أنتل وسيسكو تطرحان كروت شبكة تدعم سرعة 10 غيغابت

من فترة ليست بالبعيدة أعلنت كل من شركتي أنتل وسيسكو عن إصدارهم أول منتج لكروت الشبكة Network Device لسرعة 10 غيغابت الخاصة بأجهزة الكمبيوتر العادية Desktop وسبب كتابتي لهذا الموضوع ليس الخبر فقط بل هو السعر الخيالي لهذا المنتج والذي من الصعب تصوره أيضا لنبدأ أولا بي أنتل

Intel 10 Gigabit XF SR Server Adapter

اشهر ما يميز الكرت المقدم من أنتل دعمه لي Load Balancing, IPv6, Vlan Support Packet Filterin. والكثير من المميزات الأخرى. بالإضافة إلى دعمه لعدة أنظمة تشغيل مثل ويندوز سبعة وويندوز سيرفر 2003- وأغلب أنظمة التشغيل المفتوحة المصدر.

أما السعر الذي حددته أنتل فهو \$ 2.625.99

وهذه صورة للكرت



لتتعرف أكثر على مميزات الكرت أدخل على الرابط التالي

<http://www.cdw.com/shop/products/default.aspx?EDC=1352161>

Cisco -ASA5580-2X10GE-SR=expansion module



\$ 13.854.99

أما الكرت التي قدمته سيسكو فقد وصل ثمنه إلى يمكنك الاطلاع على مميزات هذا الكرت على الرابط التالي :

<http://www.cdw.com/shop/products/default.aspx?edc=1424619>



أصدرت مجلة FORTUNE المشهورة في عالم الأعمال تقريرها السنوي لعام 2010 حول أفضل 100 شركة يمكن العمل فيها وكالعادة سيسكو كانت من بين أفضل الشركات وأحتلت هذه السنة المركز الـ 16 في الترتيب بينما أحتلت المركز الرابع في معدل النمو بالإضافة إلى كونها في الـ 25 TOP لخمس سنوات متتالية.

ودخلت سيسكو أول مرة في الترتيب عام 1996 محتللة المركز الخامس والعشرين ومحافظة على وجودها لي اثنا عشر عام متتالية في ترتيب أفضل الشركات للعمل فيها وطبعاً هذا يدل على مدى شفافية وانفتاح هذه الشركة على العالم الخارجي

أما المراكز التي احتلتها سيسكو في الأثنا عشر سنة السابقة فكانت كالتالي

العام	الترتيب
1998	25
1999	24
2000	3
2001	3
2002	15
2003	24
2004	28
2005	27
2006	25
2007	11
2008	6
2009	6

ماهي نسخة سيسكو IOS التي أحتاجها



وكما ذكرت سابقاً أن الاختلاف بين الدلالات القديمة والجديدة هو في طريقة كتابة قسم Feature فقط لذلك سوف أشرح باقي الأجزاء مرة واحدة لأنها لا تختلف في كلا القسمين .

الجزء الخاص بي ال Platform

as5200 5200
cpa25 CiscoPro 2500
c1005 1005
c2500 25xx, 3xxx, 5100, AP (11.2 and later only)|
c2600 2600 (Quake platform)|
c2800 Catalyst 2820
c2900 2910, 2950
c3620 3620
c3640 3640
c4000 4000(11.2 and later only)|
c4500 4500, 4700
c5rsm Catalyst 5000 (RSP platform)|
c5atm Catalyst 4000 (ATM platform)|
c7000 7000, 7010 (11.2 and later only)|
c7200 7200
gs7 gateway server 7000, 7010)
igs IGS, 25xx, 3xxx, 5100, AP
mc3810 Ardent Multiservice Cisco 3810 platform
rsp 75xx
xx 4000

أرقام ورموز نراها في نسخ IOS من سيسكو ونجهل معناها ماهي وما فائدتها وماذا يعني كل رمز فيها ؟؟؟

بداية كلمة IOS تعني Internet Network Operating System وهو نظام تشغيل تم تطويره في منشآت سيسكو خصيصاً لكي تعمل عليه أجهزة سيسكو سويتشات كانت أو روترات .

والموضوع بشكل عام قد يكون للبعض مهم جداً ولللبعض غير مهم لأنه ببساطة موضوع احترافي بعض الشيء ، دعوني أولاً أعرض عليكم بعض الأمثلة :

c3640-jk9s-mz.124-16a.bin
c2600-ik9o3s3-mz.122-15.T9.bin
c7200-adventerprisek9-mz.124-4.T1.bin

رموز وأرقام كثيرة ولكل واحد منها معنى وهو الموضوع الذي سوف أتكلم عنه كيف نتحدد بأحترافية الفروق بين نسخ IOS ؟

وقبل أن أبدا يجب أن أؤنبه أن لهذا الموضوع قسمان أثنان

الأول يتحدث عن الدلالات القديمة كما هو الحال في المثال الأول والثاني

والثاني يتحدث عن الدلالات الجديدة كما هو الحال في المثال الثالث ولكي

تعرف أي النسخ تقوم باستخدامها توجه إلى موجه الأوامر وقم بتنفيذ الأمر

التالي : Show Version

```
Router1
Physical Config CLI
IOS Command Line Interface

Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8z)TS, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

Copy Paste
```

لكلا القسمين هناك قاعدة واحدة وهي تقسيم الاسم إلى أربعة أجزاء بحيث تكون على الشكل التالي : XXXX-YYYY-ZZZZ-SSSS وكل

جزء منها سوف يعطي معلومة عن النسخة بحيث

Platform=XXXX الفئة التي ينتمي إليها نظام التشغيل

Feature=YYYY سمات ومميزات كل إصدار وهو نقطة الاختلاف بين

الدلالات القديمة والجديدة

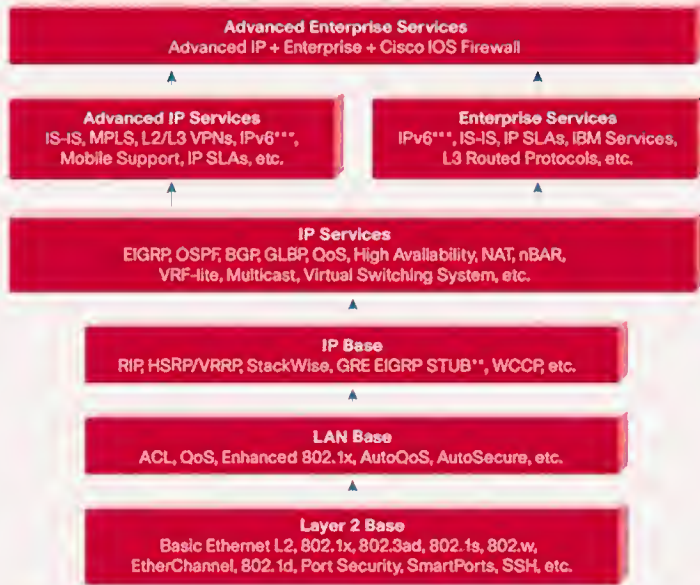
ZZZZ= تدلنا على مكان الذي يجب حفظ النظام فيه بالإضافة إلى أنها

تعطينا معلومات عن حالة نظام التشغيل هل هو مضغوط أم لا

SSSS= رقم الإصدار وعدد التحديثات التي طرأت على النسخة

XXXX YYYY SSSS
c2600-ik9o3s3-mz.122-15.T9.bin
ZZZZ

ونستطيع من خلال هذا الجسم تحديد ماتحويه كل نسخة



القسم الخاص بمكان الحفظ

f - Flash
m - RAM
r - ROM
l - relocatable
z - zip compressed
x - mzip compressed

القسم الخاص برقم الاصدار

كما ذكرت مسبقا أن هذا الجزء يدل على رقم الاصدار واذا كان هناك تحديثات جديدة تم اضافتها على نفس النسخة وسوف نفهمها بشكل أفضل في المثال العملي القادم

c2600-ik9o3s3-mz.122-15.T9.bin

القسم الاول

c2600

تدلنا على ان هذه النسخة خاصة بالروتات من Series 2600

القسم الثاني

ik9o3s3

i تدلنا على ان هذه النسخة هي IP routing version

k9 تدلنا على ان هذه النسخة هي 3DES encryption

o3 تدلنا على ان هذه النسخة تدعم الفايروول Firewall/IDS

s3 تدلنا على ان هذه النسخة هي Basic limited routing

القسم الثالث

mz معناها انها تحفظ على ال RAM وهي مضغوطة Compressed

القسم الرابع

12.2 تدلنا على ان اصدار هذه النسخة هو 12.2

15 تدلنا على عدد التحديثات التي طرأت على النسخة

T9 عدد ال Feature الجديدة التي تم اضافتها الى النسخة الاساسية

أمثلة على النسخ ذات الدلالات الجديدة وهي لا تحتاج لشرح

c7200.adventerpriseik9.mz.124.4.T1.bin

c2900-layer2basek9.mz

القسم الخاص بي ال Feature

سوف أطرح أولا معاني الدلالات القديمة وهي كالتالي :

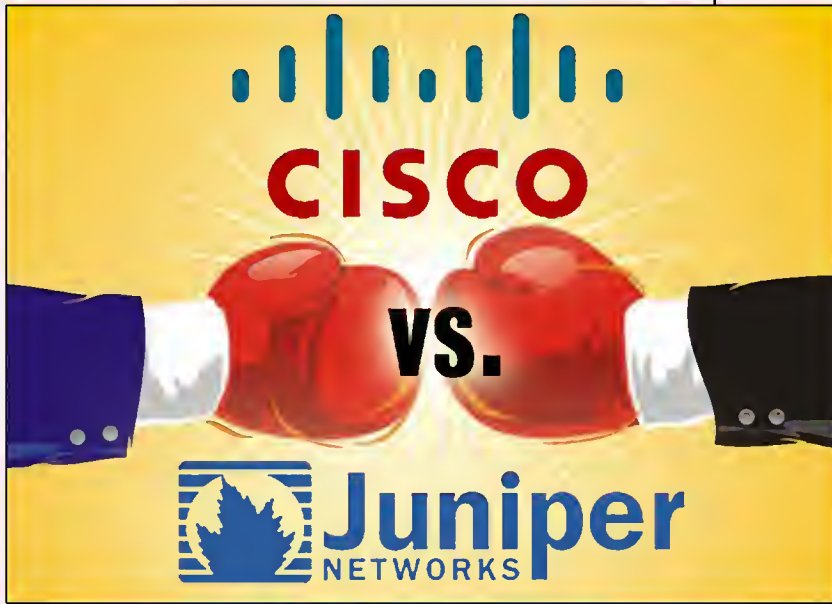
a - APPN
a2 - ATM
b - Appletalk
boot - used for boot images
c - Comm-server/Remote Access Server(RAS)
c2 - Comm-server/Remote Access Server(RAS)
d - Desktop subset (SNMP, IP, Bridging, WAN, Remote Node, IPX, AT, ARAP)
d2 - reduced Desktop subset (SNMP, IP, IPX, AT, ARAP)eboot
f - FRAD subset (SNMP, FR, PPP, SOLL, STUN)
f2 - modified FRAD subset (EIGRP, Pcbus, Lan Mgr, removed, OSPF added)
g - ISDN subset (SNMP, IP, Bridging, ISON, PPP, IPX, AT)
g2 - gatekeeper proxy, voice and video
i - IP subset(SNMP, IP, Bridging, WAN, Remote Node, Terminal Service)
i2 - subset similar to IP subset for system controller image(3600)
i3 - reduced IP subset with BGP/MIB, EGP/MIB, NHRP,
j - enterprise subset (formerly bpx, includes protocol translation)
k - kitchen sink (enterprise for high-end)
l - IPExchange IPX, static routing, gateway
m - RMON (11.1 only)
n - IPX
o - Firewall (Formerly IPExchange Net Management)
p - Service Provider (IP RIP/IGRP/EIGRP/OSPF/BGP, CLNS, ISIS/IGRP)
p2 - Service Provider w/CIP2 ucode
p3 - AS5200 service provider
p4 - 5800(Nitro) service provider
q - Async
q2 - IPExchange Async
r - IBM base option (SRB, SOLL, STUN, OLSW, QLLC) - comes with i, in, d
r2 - IBM variant for 1600 images
r3 - IBM variant for Ardent images (3810)
r4 - reduced IBM subset with (BSC/MIB, BSTUN/MIB, ASPP/MIB, RSRB/MIB)
s - source route switch (SNMP, IP, Bridging, SRB) (10.2 and following)
s - (11.2 only) addition to the basic subset (Plus version)
t - (11.2)AIP w/ modified Ucode to connect to Teralink 1000 Data
u - IP with VLAN RIP (Network Layer 3 Switching Software, rsr, srt, srb, sr/tlb)
v - VIP and dual RSP(HSA) support
w - Reserved for WBU
w2 - Reserved for CiscoAdvantage ED train
w3 - Reserved for Distributed Director
x - X.25 in 11.1 and earlier release
y - reduced IP (SNMP, IP RIP/IGRP/EIGRP, Bridging, ISON< PPP) (C1003/4)
- reduced IP (SNMP, IP RIP/IGRP/EIGRP, Bridging, WAN - X.25) (C1005)
(11.2 - includes X.25) (C1005)
y - IP variant (no Kerberos, Radius, NTP, OSPF, PIM, SMRP, NHRP...) (C1600)
y2 - IP variant (SNMP, IP RIP/IGRP/EIGRP, WAN - X.25, OSPF, PIM) (C1005)
y2 - IP Plus variant (no Kerberos, Radius, NTP...) (C1600)
y3 - IP/X.31
Y4 - reduced IP variant (Cable, Mibs, OHCP, EZHTTP)
z - managed modems
40 - 40 bit encryption
56 - 50 bit encryption
56i - 56 bit encryption with IPSEC

الدلالات الجديدة وفيها تم اختصار كل هذه الرموز إلى ثمانية كلمات فقط وهي

IP Base
IP Voice
Enterprise Base
Advanced Security
SP Services
Advanced IP Services
Enterprise Services
Advanced Enterprise Services

مقارنة بين سيسكو وجونيبر

قد يتفق معي الجميع على أن مقارنة شيان كبيران شيء صعب جدا مثل أن نقارن بين ويندوز ولينوكس أو أن نقارن بين جونيبر وسيسكو والسبب طبعا أن لكل منتج منهم سلبياته وإيجابياته ومميزاته مما يجعل الموضوع أصعب للمقارنة لذلك قررت أن أنزل درجة واحدة وأقوم بمقارنة بين نظامي التشغيل المستخدمين في كل من أجهزة جونيبر وأجهزة سيسكو أي بين نظامي JUNOS و IOS



أما بالنسبة لي JUNOS من جونيبر

ولد جونوس في عام 1996 أي بعد IOS بعشرة سنوات وهو يعد كنظام Modular operating system تم اعداده لكي يعمل على نظام تشغيل المفتوح المصدر FreeBSD وبالتالي هذا يضيف للعمليات التي تجري الخصوصية والحماية ويؤمن مساحة خاصة من الذاكرة لكل تطبيق بالإضافة إلى إمكانية تحديث النظام أو إضافة Feature جديدة في أي وقت ومن دون الحاجة إلى إزالة نظام التشغيل أو حتى إعادة تشغيله بالإضافة إلى إمكانية أخذ نسخة من الأعدادات في وقت تريد من خلال كتابة الأمر request system snapshot

وكنوع من الأمان والرونة يتطلب تنفيذ أي تغيير على الجهاز تأكيد الأمر من خلال إضافة الأمر commit والتي تضمن لك أن تنفذ كل الأوامر اللازمة وتفعيله مرة واحدة على الروتر وللعودة خطوة للوراء نكتب rollback أما أكثر ما يميز جونوس هو وجود نسخة واحدة لكل ال Platform الموجودة في جونيبر سويتش كان أو روتر وهذا يشمل J, M, MX, T, EX Series وآخر إصدار كان يحمل الرقم 10.0

وفي جونوس تستطيع تنفيذ عدة أوامر في سطر واحد فقط وهذه بعض الأمثلة : مثال على طريقة كتابة أيبي لأحد المنافذ

```
set interfaces fe0 unit 0 family inet
address 192.168.1.1/24
```

مثال آخر على الأكسس ليست

```
filter trusted-prefixes {
term controlled-access {
from {
address {
192.168.1.0/24;
128.29.31.0/24;
207.46.150.0/24;
protocol tcp;
port [ ftp telnet ssh ];
}
then accept;
}
term access-denied {
then {
log;
reject;
}
}
}
```

لنبدأ أولا بالأكثر شهرة وهو IOS من سيسكو

الأكثر من عشرين عام كان هذا النظام هو الرقم واحد في عالم الشبكات من حيث لأستخدام ويعد ال IOS كنظام من نوع monolithic operating system وترجمته تعني أنه نظام متكامل ومتناغم ومعنى هذا الكلام يعود إلى أن نظام سيسكو عندما يعمل قانه يكون كقطعة واحدة تتشارك فيه كل العمليات نفس الحيز من الذاكرة

وبسبب هذا التشارك في الذاكرة وعدم وجود حماية بين العمليات التي تجري على الذاكرة يؤدي هذا إلى حدوث خلل في جميع العمليات وفقد بعض المعلومات في حال كان هناك أي خطأ برمجي في أي عملية على الذاكرة

وبمحاولة من سيسكو لتفادي هذه المشكلة أعلنت عن إصدار جيل جديد من ال IOS تحت اسم ال IOS XR معتمدا على Third party System يدعى QNX

لتنصيب نظامها الجديد والذي يعمل في أجهزة CRS العملاقة والذي يعد Modular operating system المشابه لنظام جونوس في جونيبر بالإضافة إلى وجود نوعين آخرين يحملان الأسماء التالية IOS XE, NX-OS

وتصدر سيسكو نظام IOS مخصص لكل جهاز من أجهزته يحمل رقم ال Series الذي ينتمي إليه وهذه بعض الأمثلة

```
c3640.jk9s.mz.124-16a.bin
```

```
c7200-adventerprisek9-mz.124.4.T1.bin
```

وآخر إصدار من IOS كان يحمل الرقم 15.0 وتحتاج عملية تحديث النظام بشكل عام إلى إزالة النظام القديم بشكل كامل ووضع النظام الجديد في مكانه بالإضافة إلى اختلاف طريقة كتابة الأوامر أحيانا من نسخة لآخرى

كما يتطلب تنفيذ شيء معين كتابة كل أمر في سطر منفرد أمثلة على تطبيق بعض الأوامر :

مثال على طريقة كتابة أيبي لأحد المنافذ

```
Interface fastethernet 0/0
```

```
Ip address 192.168.1.1 255.255.255.255.0
```

```
No shutdown
```

مثال آخر على الأكسس ليست

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq ftp
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq telnet
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq ssh
access-list 101 permit tcp 128.29.31.0 0.0.0.255 any eq ftp
access-list 101 permit tcp 128.29.31.0 0.0.0.255 any eq telnet
access-list 101 permit tcp 128.29.31.0 0.0.0.255 any eq ssh
access-list 101 permit tcp 207.46.150.0 0.0.0.255 any eq ftp
access-list 101 permit tcp 207.46.150.0 0.0.0.255 any eq telnet
access-list 101 permit tcp 207.46.150.0 0.0.0.255 any eq ssh
```


نتائج الاستفتاء الشهري

نتائج الاستفتاء

هل أنت من متابعي مواضيع جونيبر ؟

• نعم

38%

• لا

33%

• حسب الموضوع

28%

الاستفتاء الأخير الذي قمت به على المدونة كان حول معرفة عدد متابعي مواضيع جونيبر والنتائج للأسف الشديد كانت مؤسفة جدا فقد وصل عدد المصوتين إلى 40 مصوت فقط وكانت النتائج كما هو واضح عندكم متقاربة جدا ويتضح لي من خلال هذه النسب أن الأغلبية لاتعطي جونيبر أي أهمية لأن الخيار الثالث يعني أن المصوت من الممكن أن يقرأ الموضوع لوفي حال أعجبه عنوان الموضوع أو المقدمة وهذا يدل على عدم الاهتمام بجونيبر والسبب برائي يتلخص في عدة أسباب من أهمها :
أ- جهل أو عدم معرفة بالشركة وهذا أتضح معي من خلال المدونة وبعض المنتديات فقد وجدت الكثير من الأشخاص الذي لم يسمح بشركة تدعى جونيبر أبدا ولم يسمح أيضا أن هناك شركة منافسة لسييسكو في عالم الشبكات

ب- قلة الشركات التي تدعم أجهزة جونيبر وبالتالي هذا ينعكس سلبا على نسبة الوظائف المتاحة وقد تم شرح هذا السبب في موضوع تعرف على منتجات جونيبر

ج- محاولة التخصص في شيء معين مثل أجهزة سييسكو فقط وهو برائي شيء صحيح وغير صحيح لماذا صحيح لأنني من مناهضي أن يكون للمهندس توجهات واحدة وفي شيء معين وفي نفس الوقت أرى أن الاطلاع شيء إيجابي جدا بالإضافة إلى أن جونيبر تعتمد على أسلوب مختلف عن سييسكو بعض الشيء

د- أخيرا عدم وجود محاكيات قوية تعطي نتائج مقبولة للشخص المتدرب وبعكس سييسكو التي وفرت برنامج الباكيت ترايسير بالإضافة لوجود برنامج الجي أن أس الذي يعطي نتائج جيدة جدا للمتدرب في المقابل جونيبر تملك محاكي واحد ونتأجه لاتعطي الحد المطلوب للتدرب



شجع هذا النوع من المجلات بوضع أعلاناتك هنا

تعرف على كيفية كتابة الأوامر في JUNOS

سوف أحول في هذه المقالة أن أقرب للمستخدم العربي كيفية العمل على نظام التشغيل الخاص بجونيبر والذي يسمى JUNOS أو جونس من خلال شرح بعض الأوامر البسيطة والمعروفة عند الجميع والتي تشمل أوامر تغيير أسم الروتر وكيفية وضع كلمة سر وأعطاء أيبي للمنفذ بالإضافة الى بعض الأوامر الأخرى

ولعرض النتائج سوف أقوم بكتابة الأمر التالي

```
root@R1# show system
host-name R1;
root-authentication {
  encrypted-password HZW.6wQBKjb.I; ## SECRET-DATA
}
login {
  user ayman {
    uid 2000;
    class super-user;
    authentication {
      encrypted-password "$1$l0FHF2gZ$9I2h36Bf1.Ue2Q1Re2Vya1";
    }
  }
}
```

الأمر التالي هو أعطاء المنفذ أيبي

```
Juniper's JUNOS
root@R1# set interfaces em0 unit 0 family inet address 192.168.1.1
/24
[edit]
Root@R1# commit
```

لعمل LoopBack Interface نقوم بتغيير بسيط في الأمر

```
Juniper's JUNOS
root@R1# set interfaces lo0.1 family inet address 192.168.100.100/24
[edit]
Root@R1# commit
```

والأمر التالي لعرض جميع المنافذ الموجودة على الجهاز

```
root@R1> show interfaces terse
Interface      Admin Link Proto  Local                Remote
dsc            up      up
em0            up      up
em0.0          up      up      inet    192.168.1.1/24
em1            up      up
em1.0          up      up      inet    192.168.3.1/24
gre            up      up
ipip           up      up
lo0            up      up
lo0.1          up      up      inet    192.168.100.100/24
lo0.16384      up      up      inet    127.0.0.1
lo0.16385      up      up      inet
lo0.32768      up      up
ls1            up      up
mtun           up      up
pimd           up      up
pime           up      up
tap            up      up
```

أمر إضافة Default Route للشبكة

```
Juniper's JUNOS
root@R1# set routing-options static route 0.0.0.0/0 next-hop
192.168.3.1
[[edit]
Root@R1# commit
```

ولعرض الـ Routing Table نقوم بكتابة الأمر التالي

```
root@R1> show route terse
inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
A Destination      P Prf Metric 1 Metric 2 Next hop      AS path
* 192.168.1.0/24    0 0      0 0      >em0.0        Local
* 192.168.1.1/32    0 0      0 0      >em1.0        Local
* 192.168.3.0/24    0 0      0 0      >em1.0        Local
* 192.168.3.1/32    L 0      0 0      >lo0.1        Local
* 192.168.100.0/24  0 0      0 0      >lo0.1        Local
* 192.168.100.100/32 L 0      0 0      Local
* 224.0.0.5/32     0 10     1 0      MultiRecv
__juniper_private2__inet.0: 1 destinations, 1 routes (0 active, 0 holddown, 1 hidden)
```

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

Juniper[®] NETWORKS

JUNOS[®] SOFTWARE

بداية وقبل كل شيء سوف نقوم بكتابة كلمة CLI للدخول على موجه الأوامر والتي تقابلها في سيسكو كلمة Enable

الأمر الأول الذي أريد التحدث عنه هو طريقة تغيير أسم الروتر أو مايعرف بي الـ Host name

```
Juniper's JUNOS
root> configure
Entering configuration mode
root# set system host-name R1
root# commit
commit complete
```

الأمر الثاني طريقة أعداد التوقيت والتوقيت

```
Juniper's JUNOS
root@R1> set date 201003280901.10
Mon Mar 28 09:01:10 UTC 2010
```

الأمر الثالث طريقة تغيير كلمة السر في حساب المدير

```
Juniper's JUNOS
root@R1# set system root-authentication plain-text-password
New password:
Retype new password:
root@R1# commit
commit complete
```

الأمر الرابع كيفية إضافة مستخدم جديد

```
Juniper's JUNOS
root@R1# set system login user ayman class super-user
authentication plain-text-password
New password:
Retype new password:
[edit]
Root@R1# commit and-quit
```

لتبسيط هذا الأمر قليلا قمت أولا بتحديد أسم المستخدم وبعدها قمت بتحديد نوع الصلاحيات التي سوف يأخذها المستخدم من خلال كتابة كلمة Class وبعدها قمت باختيار أحد الصلاحيات المتاحة والمبينة في الجدول التالي

Class	Permission
operator	clear network reset trace view
read-only	view
super-user	all
unauthorized	none

مواضيع متفرقة

DEFAULT INTERFACE

```
Current configuration : 134 bytes
!
interface FastEthernet0/0
description this interface connect to data server
switchport access vlan 2
spanning-tree portfast
end
```

```
Current configuration : 33 bytes
!
interface FastEthernet0/0
end
```

SUBNET /31 ؟

Default Interface

حقيقة الـ Subnet /31 ؟

لموضوعي هذا له ثلاث مميزات بسيطة وسريع ومهم جدا وهو امر يمكنك استخدامه في اجهزة سيسكو وهو Default Interface يقوم هذا الامر بالغاء كل الاعدادات لتى قمت بها على اي Interface ويرجعه الى حالته الاولى وكمثال صغير على هذا الموضوع سوف اقوم بعرض احد الـ البورتات كما في الصورة التالية

```
Router# sh run interface fastEthernet 0/0
Building configuration...

Current configuration : 134 bytes
!
interface FastEthernet0/0
description this interface connect to data server
switchport access vlan 2
spanning-tree portfast
end

Router#
Ready Telnet 24, 8 24 Rows, 66 Cols VT100
```

وكما تشاهدون قمت بتنفيذ عدة أوامر على البورت ولكي اقوم بالغاءها يجب علي أن اقوم باضافة كلمة no قبل كل امر لكي اقوم بالغاءها وهذا سوف يستغرق بعض الوقت والجهد في حال كان هناك الكثير من البورتات والكثير من الاعدادات لذلك سوف اقوم بكتابة الامر التالي

default interface fastEthernet 0/0

في الـ Global mode وهو بدوره سوف يزيل كل الاعدادات الموجودة وسوف يرجع البورت الى حالته الاولى وهذه صورة للتوضيح

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#default interface fastEthernet 0/0
Building configuration...

Interface FastEthernet0/0 set to default configuration
Router(config)#exit
Router# sh run interface fastEthernet 0/0

Building configuration...

Current configuration : 33 bytes
!
interface FastEthernet0/0
end

Router#
Ready Telnet 26, 8 26 Rows, 61 Cols VT100
```

ثناء وجودي على موقع ويكيبيديا اثارني موضوع الـ Subnet 31 ما اهميته وهل يستخدم في الحياة العملية ؟

وحقيقة انا تعودت دائما عندما اقوم باي اعداد لاحد البورتات ان اعطي البورت الـ Mask 30/ ولم يخطر على بالي ان اقوم بتجربة الماسك 31 لان

باعتقادي هذا الماسك غير صالح

وبعد التجربة اتضح انه يمكنك استخدام هذا الماسك بكل بساطة ويعد استخدامه شائع جدا وهو يستخدم فقط في حالة كان الربط بين Point-to-Point

في شبكات الـ Wan الواسعة

والهدف الاول والآخر منه هو المحافظة على اكبر قدر ممكن من الـ Public IP المتاحة للاستخدام الخاص

واحب ان اضيف ان هذا النوع لايملك عنوان خاص للـ Broadcast وهو في هذه الحالة يقوم بتحويل البايت الى الايبي الثاني بشكل أوتوماتيكي

وقد قامت سيسكو باضافته اول مرة الى اجهزته في النسخة 12.2(2)T

ويتطلب منك ان تقوم باضافة امر صغير بعد كتابة الايبي وهو

```
interface Serial5/1
```

```
ip address 192.168.1.0 255.255.255.254
```

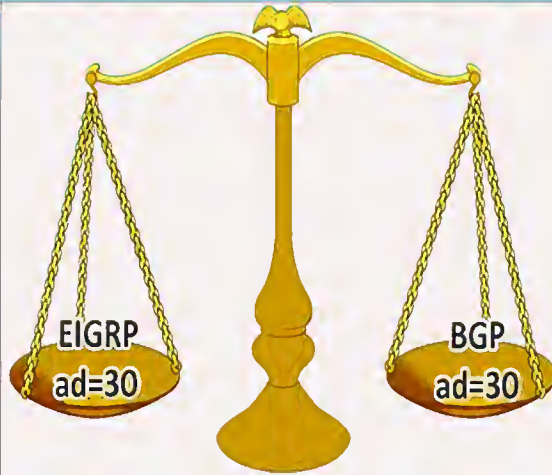
```
no ip directed-broadcast
```

```
no shutdown
```

ولو في حال كنت تستخدم اصدار احدث من 12.2 فانت لست بحاجة لكتابة الامر السابق تستطيع ان تقوم بتجربته على الـ GNS3



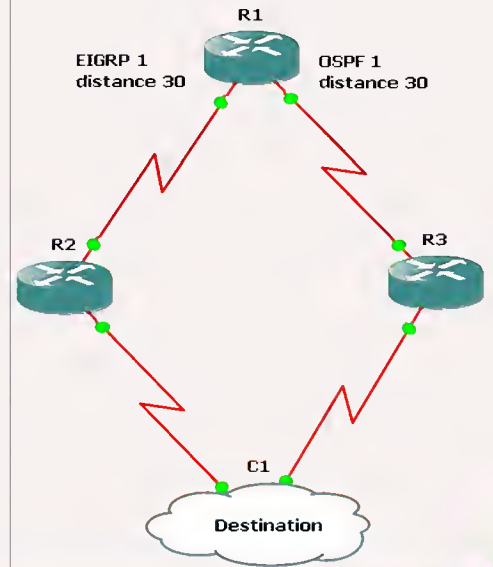
ماذا سوف يختار الروتر لو كان لديه بروتوكلان مختلفان اهم نفس AD



منذ فترة ليست ببعيدة خطر على بالي سؤالين الأول: ماذا سوف يحدث لو كان الروتر يملك مسارين مختلفين لنفس الهدف وعلى كل مسار تم أعداد Routing Protocol مختلف عن الآخر؟

وطبعا الجواب بسيط جدا وهو من يملك AD Administrative Distance أقل هو من سوف يفوز وسوف يستخدمه الروتر للاتصال مع الهدف والسبب ببساطة لأننا الروتر لا يسمح لأكثر من بروتوكول للعمل في نفس الوقت . وطبعا ليس هذا هو السؤال المهم ؟

الثاني: ماذا سوف يحدث لو كان لدينا نفس الحالة السابقة لكن قمنا بتغيير الـ AD على كل بروتوكول ؟ سوف أستعين بهذه الصورة لتوضيح الأمر



كما ترون للروتر R1 مسلكان R2 & R3 لكي يصل للهدف المنشود وقد قمت بتغيير الـ AD لكل بروتوكول من خلال الأوامر التالي

```
R1(config)# router eigrp 1
R1(config-router)# distance 30
R1(config-router)# router ospf 1
R1(config-router)# distance 30
```

طبعا باقي أعدادات البروتوكول لم أكتبها لأنها ليست محور حديثنا وهي معروفة عند الجميع المهم عندما قمت بعرض الـ Routing Table من خلال الأمر Show IP Route وجد أن الـ Eigrp هو الذي مازال المسيطر على الروتر ، وللوهلة الأولى ظننت أن هذا حدث بسبب أستخدامي لروتر من نوع سيسكو بالإضافة إلى أنني تأكدت أن بروتوكول الـ OSPF مازال يعمل وذلك بقطع الاتصال مع الروتر الذي يعمل بواسطة الـ Eigrp

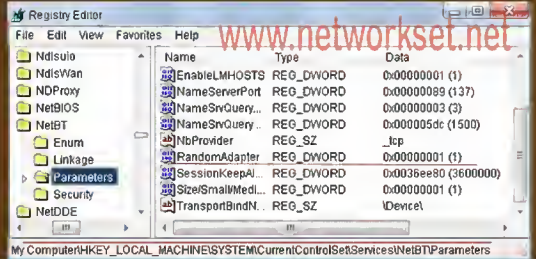
ولكي أصل إلى حقيقة الأمر قمت بعمل تجربة أخرى لكن هذه المرة بين الـ BGP و Eigrp ووجدت أن الـ BGP هو من أخذ المسار للوصول الى الهدف وبعد البحث والتدقيق توصلت الى هذه النتيجة وهي عندما يكون لدينا بروتوكلان يعملان على روتر ولهم نفس الـ AD يقوم الروتر وبشكل أوتوماتيكي بالأختيار حسب الـ AD default لهم أي يعود إلى فكرة السابقة وهي من أقل هو الذي سوف يفوز وهذا الجدول يوضح قيمة الـ AD default لكل البروتوكولات المتاحة على الشبكة

Route Protocol	Default AD
interface Connected	0
route Static	1
EIGRP summary route	5
BGP External	20
EIGRP Internal	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
On Demand Routing (ODR)	160
EIGRP External	170
BGP Internal	200
* Unknown	255

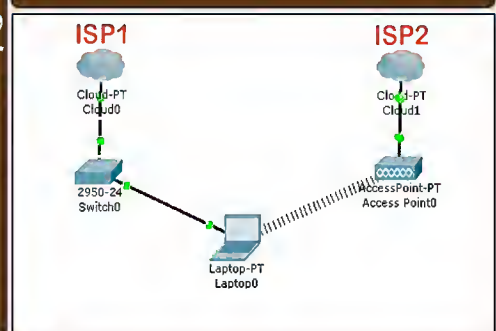
منذ حوالي اليومين قدمت إحدى شركات مخدومي الأنترنت في المنطقة التي أعيش فيها خدمة **Wireless** بشكل مجاني ولمدة شهرين وطبعا قمت بالاشتراك فيها من خلال جهاز المحمول مع العلم أنني لدي خط أنترنت واصل للبيت من خلال سويتش وهنا خطراً على بالي شيء مهم وهو هل يمكن أن أقوم بعمل **Load Balancing** بين شركتي الأنترنت؟؟؟

والهدف طبعا تخفيف الحمل وزيادة الأداء وبعد البحث لخمس دقائق على غوغل وجدت أن الموضوع ممكن وبسيط جدا وكل ما عليك أن تفعله هو أن تفتح الريجستري وتنتج إلى المكان التالي
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
وبعدها أضغط بالزر اليميني وقم بأختيار **NEW** وبعدها أختار **DWORD Value** وقم بإعادة تسميته إلى **RandomAdapter** وتعطيه القيمة واحد كما هو موضح بالصورة

وبعدها قم بعمل إعادة إقلاع للويندوز ومبروك عليك وتمت تجربة هذه الطريقة على ويندوز **XP** وتقوم الـ **Load Balancing** في ويندوز على فكرة أختيار كرت شبكة عشوائي في كل مرة تطلب فيها شيء من الأنترنت



كيف تقوم بعمل Load Balancing على ويندوز





قسم أمن وحماية الشبكات

هذا القسم سوف يتم عرض فيه كل الأمور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التي تحدث على الشبكة وأرجو منكم أن تدقق على كلمة تخفيف لأن النظرية العامة تقول لا يوجد جهاز آمني خالي من الثغرات مهم كانت قوته!



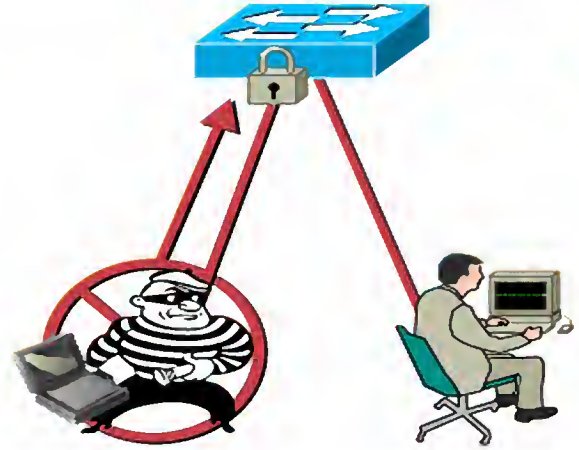
هجوم الـ Mac Flooding وطريقة التصدي له

ما هو الهجوم الـ MAC Flooding ؟

فكرة هذا الهجوم ببساطة هو تحويل السويتش إلى هوب ويتم هذا الأمر بإرسال عدة فريمات تحوي عناوين ماك أدريس مزورة إلى السويتش بهدف جعل الماك أدريس تايليل تمثلاً.

لأننا نعلم أن للماك أدريس هناك حدود معينة لعدد العناوين التي من الممكن تسجيلها على التايليل.

وبعد أن تمثلاً التايليل يتحول السويتش ببساطة إلى الهوب وسبب تحوله إلى هوب هو عدم قدرته السويتش على تسجيل العناوين الجديدة القادمة من غير منافذ مما يطر السويتش في كل مرة يستلم فيها أي فريم إلى إرسالها إلى جميع المنافذ المتاحة وبهذه الطريقة يستطيع المهاجم التتصّل على جميع الفريمات التي تمر عبر السويتش بأي برنامج يقوم بتحليل البيانات وبمعنى آخر يتحول هذا الشخص إلى Man in the middle



وبكلام آخر أول ماك أدريس سوف يتصل على البورت سوف يكون هو الوحيد القادر على الاتصال بالسويتش وهو يشيدنا في موضوع ردع هجوم الـ Mac Flooding وفي حال لو أردنا أن نسمح لأكثر من ماك أدريس للاتصال بالسويتش نكتب الأمر التالي

```
Switch(config-if) # switchport port-security maximum 3
```

وقد سمحت هنا بي 3 أجهزة للدخول إلى السويتش من خلال هذا البورت وفي حال لو أردت أن أقوم بتحديد ماك أدريس معين هو الوحيد الذي يستطيع الدخول إلى السويتش أقوم بكتابة الأمر التالي مع إضافة رقم الماك أدريس

```
Switch(config-if) # switchport port-security mac-address 00-11-22-33-44-55-66
```

ولو وجدت أن هذا الموضوع مرهق وطويل جداً تستطيع أن تضع مكان كل ماك أدريس كلمة Sticky وهي تخبر السويتش بتسجيل الماك أدريس المتصل حالياً على البورت كـ Static Mac Address وصيغة الأمر تكون

```
Switch(config-if) # switchport port-security mac-address mac-address sticky
```

وأخيراً لتغيير ردة الفعل التي سوف يتخذها السويتش في حال تم حدوث أي تجاوز نكتب الأمر التالي

```
Switch(config-if) # switchport port-security mac-address violation ?
```

ونختار أحد الخيارات الثلاث الموضحة في الجدول السابق

ولاستعراض حالة البورتات على السويتش نقوم بكتابة الأمر التالي

```
Switch#show port-security address
```

Switch#show port-security address				
Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	000A.4145.6254	DynamicConfigured	FastEthernet0/1	-
1	000C.CFDE.C403	DynamicConfigured	FastEthernet0/1	-
1	00E0.F7DE.1C78	DynamicConfigured	FastEthernet0/3	-
1	00E0.8F2B.39B1	DynamicConfigured	FastEthernet0/4	-
Total Addresses in System (excluding one mac per port) : 1				
Max Addresses limit in System (excluding one mac per port) : 1024				
Switch#				

كما هو واضح من الصورة قمنا بالسماح للمنفذ FastEthernet 0/1 بأن يقبل أكثر من ماك أدريس وهذا بدوره يفسر لنا وجود اثنين ماك أدريس في القائمة

ما هو الـ Port Security ؟

هو وظيفة نقوم بإعدادها على كل Interface تهدف لتحديد أجهزة الكمبيوتر التي يسمح لها بالاتصال من خلال هذا الـ Interface وتتم العملية عن طريق ربط الـ Interface بالماك أدريس الخاص بكل جهاز كمبيوتر لديه الصلاحية للدخول على الشبكة وبهذه الطريقة تكون قد منعنا الأجهزة الدخيلة من المحاولة بالاتصال بالشبكة من خلال شبك الكمبيوتر بأحد مخارج السويتش كما تمكنا من ردع هجوم Mac Flood من خلال تحديد عدد الأجهزة المتصلة بالـ Interface في حال لو كان عندنا Hub مثلاً

ماذا سوف يحدث في حال محاولة أحد الأشخاص الولوج إلى الشبكة ؟
 الـ Port Security ثلاث وضعيات يمكن أن يتخذها في حال تم شبك ماك أدريس لجهاز كمبيوتر غير مصرح به للدخول إلى الشبكة والحالات هي كالتالي

Mode	Description
shutdown	في هذه الحالة سوف يقوم السويتش بإغلاق المنفذ بشكل مباشر وهذه الوضعية تعد الـ Default للـ Port Security
protect	في هذه الحالة يقوم السويتش بعمل Drop لكل الترافيك القادم من الماك أدريس الغير مصرح به مع أبقاء المنفذ مفتوح للأجهزة المصرحة بها
restrict	نفس الحالة السابقة لكن هنا يقوم السويتش بأحصاء كل الباكيث التي قام بعمل drop لها

طريقة إعداد الـ Port Security

طريقة إعدادها كما بينت في بداية الموضوع في غاية السهولة وتتم عن طريق امرين فقط

```
Switch#conf t
```

```
Switch(config)# interface fastethernet 0/1
```

```
Switch(config-if) # switchport mode access
```

```
Switch(config-if) # switchport port-security
```

كما نرى نقوم أولاً بتحديد البورت وبعدها نختار mode access لكي نخبر السويتش أن هذا البورت متصل مع end device أو جهاز كمبيوتر وعندما نقوم بتنفيذ الـ Port Security فالحالة الطبيعية التي يتخذها السويتش كما أوضحنا سابقاً هي إغلاق السويتش و السماح لي ماك أدريس في العبور عبر هذا البورت



الـ ROMmon كما يعرفه الأغلبية على أنه المكان المخصص لاستعادة كلمة السر والقيام ببعض الوظائف الأخرى يعد أيضا مكان خطرا اذا في حال تم الوصول إليه من بعض الأشخاص الحاقدين وسوف أحاول في هذه المقالة توضيح فوائد وخطورة الـ ROMmon بالإضافة إلى كيفية حماية أجهزة سيسكو من مخاطر التلاعب به والتي بدورها أيضا تشكل سلاح ذو حدين

بعد أن تعرفنا على الأماكن التي يتحياها الـ ROMmon وأيقنا أن الوصول لهذا المكان الحساس يؤدي إلى مشاكل كارثية في حال وجود أحد الأشخاص الحاقدين أو المخربين في المكان الموجود فيه الروتر وتستطيع أن تتخيل معي ماذا يستطيع أن يفعل في حال قام بتغيير كلمة السر وبعدها الدخول إلى الروتر عندها كل شيء يصبح ممكنا من التجسس على البيانات التي تمر إلى الوصول لأماكن حساسة غير مسموح له بالدخول إليها.

لذا أتاحه لك سيسكو أمر خاص تستطيع من خلاله تعطيل هذه الخدمة. وقبل أن أذكر لك هذا الأمر يجب أن تعرف أن هذا الأمر سلاح ذو حدين، فانت تستطيع تعطيل الدخول إلى الـ ROMmon لكن في حال نسيت كلمة السر فليس أمامك إلا أن تقوم بإعادة الجهاز إلى إعدادات الأصلية أي مايعرف بي Default Factory Configuration

```
Router>en
Router#conf t
Router(config)#no service password-recovery
```

وعلى فكرة لو حاولت أن تكتب في موجه الاوامر علامة الاستفهام لن تجد الأمر بكل بساطة لان سيسكو قامت بأخفائه لخطورته وهذه صورة للتوضيح

```
Router con0 is now available

Press RETURN to get started.

User Access Verification

Password:
Password:
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no service password-?
password-encryption
Router(config)#no service password-■
```

وهذه صورة توضح ماذا يحدث عند محاولة الدخول على الـ ROMmon بعد تعطيله

```
Router# configure terminal
Router(config)# no service password-recovery

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload

Proceed with reload? [confirm] yes

00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by Cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
```

يعد الـ ROMmon هو المكان الوحيد الذي نستطيع أن نلجأ له في حال حدوث مشكلة تقنية في الجهاز مثل نسيان كلمة السر أو حدوث مشكلة في نظام التشغيل وكما هو معروف عند الجميع الدخول على الـ ROMmon يتم عادة عن طريق الضغط بوقت واحد على كل من زري الـ CTRL+Break عند بداية اقلاع الجهاز سويتش كان أم روتر ولكي نستطيع أن نكتشف ماهي الاوامر التي يتيحها الـ ROMmon سوف نقوم بعرض الاوامر من خلال كتابة الأمر Help أو من خلال وضع علامة الاستفهام في موجه الاوامر "؟"

```
System Bootstrap, Version 12.3(8)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
#####
monitor: command "boot" aborted due to user interrupt
rommon 1 > help
boot                boot up an external process
confreg             configuration register utility
dir                 list files in file system
help               monitor builtin command help
reset              system reset
set                display the monitor variables
tftpdnld            tftp image download
unset              unset a monitor variable
rommon 2 >
```

كما نلاحظ من الصورة أن الـ ROMmon عدة مهام يستطيع أن يقوم بها وهذه المهام تختلف حسب طبيعة الجهاز فهي تزيد أو تنقص بشكل عام والـ الاوامر المتاحة على الصورة تعد هي الأهم في استخدام الـ ROMmon والتي سوف أقوم بشرح كيفية استخدامها وسوف نبدأ حسب التسلسل

Boot لكي نقوم بالاغلاق من خلال الـ IOS الموجودة على الفلاش بصورة طبيعية من خلال الأمر boot flash وطبعا الروتر سوف يأخذ أول نسخة موجودة على الفلاش وفي حال أردنا أن نقوم بالاغلاق من قسم آخر على الفلاش نقوم بكتابة

boot flash:2

Confreg لكي نقوم بتغيير قيمة الريجستري وهو أمر مهم لاستعادة كلمة السر ومثال عليه

confreg 0X2142

Dir لعرض الملفات الموجودة على الفلاش ويتم من خلال كتابة الأمر

dir flash

Help لعرض الاوامر الممكنة كما تم ذكره من قبل

Reset لكي نقوم بإعادة الاقلاع

Set لكي نقوم بإعداد الـ Tftp Server ويتم إعدادها على الشكل التالي:

```
set tftpabc IP Add Mask Default GW IP tftp server
set tftpabc 10.10.0.0 255.0.0.0 10.1.1.0 10.29.32.0
```

Tftpdnld من أجل تحميل نسخة IOS من سيرفر الـ TFTP

Unset وهو عكس الأمر السابق ويهدف إلى إلغاء الإعدادات التي قمنا بها

عتاك و محلومات

أعداد عثمان إسماعيل

CISCO SYSTEMS



RAM	128 MB(installed)/384 MB(MAX)-SDRAM
Flash memory	32 MB(installed)/128 MB (MAX)
Type	DSL modem
MAX Transfer Rate	24 MBps
Encryption Algorithm	DES , Triple DES , AES
Supplied OS	CISCO IOS
Digital Signaling Protocol	ADSL , ADSL2 , ADSL2+
DCP	Ethernet , Fast Ethernet
Protocol Remot	SNMP
Interfaces	2 x network -Ethernet 10Base - T/100Base -TX - RJ-45 1 x management - console - RJ - 45 Serial - auxiliary - RJ-45 1 x modem ADSL
MAX Temp 40 C , MIN Temp 0 C , VPN Support , support IP Sec ,	



Router1841-ADSL

RAM	64 MB
Flash memory	32 MB
Ramer Table of MAC Addr	8 K entries
Authentication method	RADIUS , TACACS+ , Secure SHELL v.2
Interfaces	48 x network - Ethernet - RG 45
Connection Type	Hulf-duplex , Full-duplex
Data Rate	1 Gbps
DCP	Ethernet , Fast Ethernet , Gigabit Ethernet
Protocol Remote	SNMP1 , RMON , Telnet , SNMP3 , SNMP2c
Number of Ports	48 x Ethernet 10Base -T , Ethernet 100Base - TX , Ethernet 1000Base -T
MAX TEmP 40 c , MIN Temp 0 c , DHCP Support , VLAN Support , IGMP snooping , auto MDI/MDI-X , DHCP snooping	



SWITCH WS-C2960G

RAM	128 MB (installed) / 483 MB (max)
Flash memory	64 MB (installed) / 128 MB (max)
Protocol Remote	SNMP 3
Type	DSU/CSU
Interfaces	2 x network - Ethernet 10Base-T/ 100Base-TX - RJ-45 1 x USB 1 x network - auxiliary 1 x management - console
Encryption	DES, Triple DES, AES
Supplied OS	Cisco IOS
OS Required	Microsoft Windows 98 Second Edition
DCP	Ethernet, Fast Ethernet
MPLS support , min temp 0 °C , max temp 40 °C, Humidity 10 - 85%	



Router 2801



Juniper®

NETWORKS

Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
<ul style="list-style-type: none"> * Junos Software Version Support: Junos Software 9.1 * Firewall Performance (Large Packets): 750 Mbps * Firewall Performance (IMIX): 500 Mbps * Firewall and Routing PPS (64 Byte): 200,000 pps * 3DES and SHA-1 VPN Performance: 160 Mbps * Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512 * Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K * New Sessions/Second: 5,000 * Maximum Security Policies: 2048 (1 GB DRAM) 	<ul style="list-style-type: none"> * Fixed I/O: 4 x 10/100/1000 * Maximum PIM Slots: 5 * Maximum EPIM Slots: 0 	<ul style="list-style-type: none"> * BGP, OSPF, RIP, Static, ECMP: Yes * Multicast, PIM SM, SSM, IGMP: Yes * Maximum Number of Security Zones: 50 * Maximum Number of VLANs: 256 * PPP, FR, MLPP, MLFR, HDLC: Yes

Router J2350



<ul style="list-style-type: none"> * ScreenOS version tested: ScreenOS 6.2 * Firewall Perf (Large Packets) 1+ Gbps * Firewall Performance (IMIX) 1 Gbps * Firewall Packets Per Second 600,000 PPS * 3DES+SHA-1 VPN Perf 600 Mbps * Concurrent VPN Tunnels 1,000 	<ul style="list-style-type: none"> * Max Concurrent Sessions 256,000 * New Sessions/Second 15,000 * Max Security Policies 4,000 * Max Security Zones 60 * Max Virtual Routers 16 * Max Virtual LANs 150 	<ul style="list-style-type: none"> * Fixed I/O 4x10/100/1000 * Mini-Physical Interface Module Expansion Slots 0 * Physical Interface Module Expansion Slots 2 * Enhanced PIM (EPIM) Expansion Slots :4
---	---	--

Switch SSG-550M



Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
<ul style="list-style-type: none"> * Junos Software Version Support: Junos Software 9.1 * Firewall Performance : 2 Gbps * Firewall Performance (IMIX): 1 Gbps * 3DES and SHA-1 VPN Performance: 1 Gbps * Concurrent VPN Tunnels : 1 GB / 2 GB DRAM * Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 256 K / 256 K * Maximum Security Policies: 5192 (1 GB DRAM) 	<ul style="list-style-type: none"> * Fixed I/O: 4 x 10/100/1000 * Maximum PIM Slots: 6 * Maximum EPIM Slots: 4 	<ul style="list-style-type: none"> * BGP, OSPF, RIP, Static, ECMP: Yes * Multicast, PIM SM, SSM, IGMP: Yes * Maximum Number of Security Zones: 50 * Maximum Number of Virtual Routers: Yes * Maximum Number of VLANs: 1024 * PPP, FR, MLPP, MLFR, HDLC: Yes

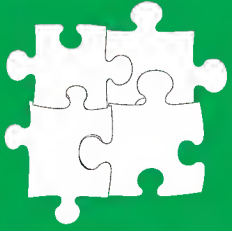
Router J6350



Data Rate <ul style="list-style-type: none"> * EX2200-24P/24T: 56 Gbps * EX2200-48P/48T: 104 Gbps Throughput <ul style="list-style-type: none"> * EX2200-24P/24T: 42 Mpps (wire speed) * EX2200-48P/48T: 77 Mpps (wire speed) 10/100/1000BASE-T Port Densities <p>24 / 48 per platform</p>	100BASE-FX / 1000BASE-X (SFP) Port Densities <p>4 per switch (fixed ports, SFP required)</p> Resiliency <p>Integral power supply and fans</p> Power Options <ul style="list-style-type: none"> * 24T and 48T (non-PoE): Autosensing; 100-120 V / 200-240 V; AC 100 W * 24P and 48P (PoE): Autosensing; 100-120 V / 200-240 V; AC 550 Operating System <p>JUNOS</p> QoS Queues / Port <p>8</p>	MAC Addresses <p>8,000</p> Jumbo Frames <p>9216 Bytes</p> IPv4 Unicast / Multicast Routes <p>6,500 / 0</p> Number of VLANs <p>1,024</p>
---	--	---

Switch EX2200





مصالحات تقنية

IANA: أو ايانا وتعني Internet Assigned Numbers Authority وهي منظمة عالمية مسؤولة عن عملية إدارة وتوزيع الأيبيات بالإضافة إلى بعض الوظائف الأخرى مثل الإشراف على Domain Name Server أو DNS وأدارة بعض معاملات البروتوكولات أو كما تعرف في لغتها Protocol Parameter ومثال عليها URL . ويقع المقر الرئيسي للمنظمة في الولايات المتحدة الأمريكية وهي تدار من قبل منظمة ايكاب أو Internet Corporation for Assigned Names and Numbers

Mac Address: ماك أدريس وتعني Media Access Control Address وهي سلسلة مرقمة وغير مكررة يتم وضعها على كل كرت شبكة من قبل الشركة المصنعة وتكتب بلغة الهيكسادسميل أي أنها تحوي الأرقام من 0 - 9 بالإضافة إلى الأحرف التالية A, B, C, D, E, F وهذا مثال عليها 00-13-22-AF-78-B1 وهي أرقام ثابتة ولا يمكن تغييرها أبدا وتشرف منظمة IEEE على توزيع الأرقام على الشركات المصنعة لكروت الشبكة NIC

RFC: وتعني Request for comments وهي سلسلة أبحاث علمية تصدر حاليا من خلال منظمة دولية تعرف بي Internet Engineering Task Force أو IETF وتشمل هذه السلسلة أبحاث ومراجع علمية تقوم بتفسير سلوكيات عمل الأنترنت و الأنظمة التي تسيرها وهي تتيح لمهندس وعلماء أجهزة الكمبيوتر بنشر أبحاثهم ضمن سلسلة منظمة وبشكل مرقم وإذا أردت الاستزادة من هذا الموضوع هناك موضوع كامل حول الـ RFC على المدونة

AppleTalk: هو أحد أنظمة الشبكات الذي قامت شركة Apple بتصميمه ونشره لمستخدمي كمبيوترات الماكنتوش MACINTOSH والذي يعد أحد الأنظمة المصنعة من قبل Apple وقد تم ضمه أول مرة في أجهزة ماكنتوش عام 1984 حتى عام 2009 عندما قررت شركة Apple التخلي عنه في إصدارها الأخير MAC OS X V10.6 لصالح TCP/IP

Routing Protocol: وتعني بروتوكولات التوجيه وهو البروتوكول المسؤول عن توجيه الاتصالات بين الروتات والذي بدوره يتيح الاتصال بين أي نقطتين على الشبكة وله عدة أنواع من أشهرها RIP, OSPF, EIGRP, BGP, IS-IS وتختلف فيما بينها بطريقة حساب أفضل مسار للوصول إلى المكان المطلوب

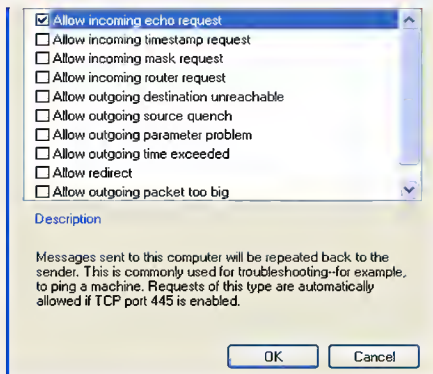
Broadcast: وهي أحد الطرق التي ينتقل فيها الترافيك في الشبكة ويتم إرسال بكل الاتجاهات المتاحة على الشبكة ويتم التعريف عنها في الشبكة بالايبي 255.255.255.255 وهي تمر عبر Hub, Switch, Bridge بينما تتوقف عندما تمر بروتروا فريم ريلاي

IP: وهي تختصر إلى Internet Protocol وتعني بروتوكول الأنترنت وهي تكون على شكل عناوين مرقمة ولها إصداران الإصدار الرابع والإصدار السادس وتبدأ الأيبيات في الإصدار الرابع من 0.0.0.0 وتنتهي بي 255.255.255.255 ووظيفتها الأساسية تأمين الاتصال لأجهزة الكمبيوتر على شبكة الأنترنت وقد تم تصنيفها إلى خمس تصنيفات A, B, C, D, E وهي تدار من قبل منظمة ايانا كما تم ذكر ذلك مسبقا

مشاكل وحلول

سوف يتم تخصيص هذا القسم لعرض المشاكل التي قد تواجهك في الشبكة بالإضافة إلى طريقة حل المشكلة كما أرحب أيضا بارسال مشاكلكم على بريد المجلة magazine@networkset.net للنظر فيها وتقديم أفضل الحلول لها .

مشكلة : لماذا الـ PING لا يعمل في شبكة مؤلفة من جهازين كمبيوتر وقد تم التأكد من طريقة التوصيل وأرقام الأيبي؟



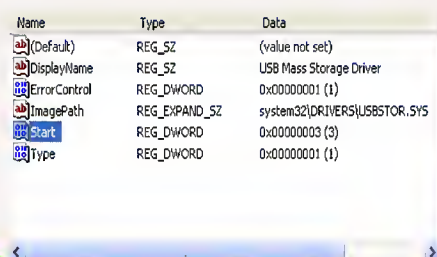
الحل : هذا النوع من المشاكل يحدث غالبا بسبب وجود الجدار الناري الموجود مع ويندوز والذي يقوم بشكل أوتوماتيكي بمنع كل رسائل الـ ICMP من الدخول إلى الجهاز ولحل هذه المشكلة لدينا طريقتان الأولى وهي إيقاف عمل الجدار الناري بشكل كامل ويتم ذلك من خلال الدخول إلى لوحة التحكم وبعدها إلى إعدادات الجدار الناري ووضع المؤشر على خيار إيقاف أو OFF الطريقة الثانية تتم بأضافة Exceptions أو استثناء للجدار الناري لكي يسمح بعبور رسائل الـ ICMP ويتم الأمر من خلال التوجه أيضا إلى لوحة التحكم وبعدها إعدادات الجدار الناري وبعدها نضغط على خيارات متقدمة أو Advanced وبعدها نختار ICMP ونضع المؤشر كما هو موضح بالصورة على خيار Allow incoming echo request على كلا الجهازين

مشكلة : السيرفر عندي لا يفتح أغلب مواقع الحماية ومضادات الفيروس مثل Kaspersky , Norton ؟



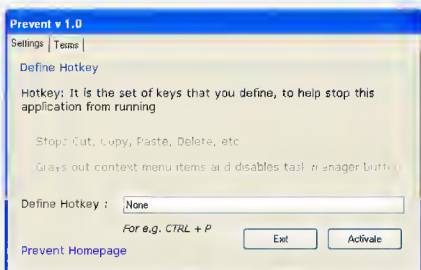
الحل : تحدث هذه المشكلة بفعل فايروس أوكراني الصنع ويدعى كونفكير أو Conficker يقوم هذا الفايروس بإغلاق أغلب مواقع الأنتي فايروس بالإضافة إلى موقع مايكروسوفت والكثير من المواقع الهامة أيضا للقضاء عليه يجب عليك أن تقوم بتحميل أداة خاصة تقوم بحذف الفايروس وتدعى Conficker Removal Tool 1.0.0.16 وهي أداة مجانية تستطيع أن تجدها من خلال استخدام البحث في غوغل

مشكلة : كيف أقوم بإغلاق كل فتحات الـ USB على جهاز الكمبيوتر ؟



الحل : قم بالتوجه إلى إبدأ أو Start وبعدها قم بالضغط على تشغيل وقم بكتابة regedit للوصول إلى مسجلات الكمبيوتر وبعدها توجه إلى العنوان التالي HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR وإبحث عن هذا التسجيل Start وقم بتغيير قيمته من 3 إلى 4 وهي تشير إلى تعطيل كل الخارج ولو في حال أردت أن تقوم بنفس الموضوع على مستوى الشبكة تستطيع أن تنفذ هذا الأمر من خلال عمل بوليسي على مستوى الشبكة

مشكلة : كيف أقوم بمنع النسخ واللصق على جهاز الكمبيوتر وعلى الشبكة أيضا ؟



الحل : لكي تقوم بإيقاف كل أشكال النسخ واللصق على جهاز الكمبيوتر لدين طريقتان الأولى الدخول على الريجستري والقيام بالتعديل على بعض المسجلات الخاصة بكل أمر والطريقة الثانية وهي أيضا تعتمد على المسجلات لكن تتم من خلال برنامج صغير جدا يدعى Prevent 1.0.0 يقوم بإيقاف كل أشكال النسخ واللصق بالإضافة إلى اختصارات لوحة المفاتيح تستطيع أن تجدها على محرك البحث غوغل .

بالنسبة لمنع النسخ على الشبكة فهي تتم من خلال سيرفر مخصص يثبت على ويندوز سيرفر و يدعى Rights Management Services وهو يقوم بأضافة صلاحيات لكل ملف من بينها صلاحيات النسخ واللصق والطباعة ويعييبها أنه لا يدعم كل أنواع الملفات الموجودة فهو يدعم ملفات الأوفيس والأدوب أكروبات وسوف يكون له موضوع كامل في المستقبل